September 2017

Issue 09

MANCHESTER
CAPITAL MANAGEMENT, LLC

Insight

The Equifax Breach

-Manchester Capital Management Strategy Group

At the risk of beating the proverbial dead horse, we would like to review the facts as we understand them related to the well-publicized Equifax breach. On September 7th, 2017, Equifax, one of the three primary credit bureaus in the country, disclosed that hackers accessed personal data belonging to 143 million people between May 13th and the end of July. In addition, credit card numbers for approximately 209,000 consumers were accessed. On August 2nd, Equifax hired FireEye's Mandiant Group, a firm known for its post-breach forensic analysis, to investigate. Mandiant informed Equifax that an initial breach occurred on March 10th, compromising customer names, addresses, dates of birth, and social security numbers. Two days prior to this breach, researchers at Cisco Systems reported a security flaw that allowed hackers to break into servers around the internet. In response, the Apache Software Foundation issued a patch to fix the security flaw in its Apache Struts web-application software, a popular software toolkit for building web services. Equifax stated that its Security organization "was aware of this vulnerability at that time, and took efforts to identify and patch any vulnerable systems." In a statement issued on September 14th, the Foundation stated that "In conclusion, the Equifax data compromise was due to their failure to install the security updates provided in a timely manner." On September 15th, Equifax announced that the Chief Information Officer and Chief Security Officer were retiring, effective immediately. More internal and external investigations are sure to follow.

In summarizing the event, Louis Hyman[1], a consumer-credit historian at Cornell University, said, "Credit bureaus are the tracks that the [credit] trains run on, and we should make sure those roads and tracks are sound if we're going to run a whole economy over them." Other bureaus have moved to spread out personal data in different places to decrease the risk that a single breach can access all a consumer's information.

Unknown at this point is the possible effect on credit creation. As consumers freeze their credit in response to the breach, will this impact the demand for credit or will consumers simply "unlock" their profiles when wishing to take out a loan or apply for a credit card? Will consumers have trouble applying for loans and passing background checks if their personal information has been compromised? What about using stolen social security numbers to file false tax returns or misappropriate benefit checks? We will closely monitor these potential effects.

There may be an investment opportunity in cyber-security firms (such as FireEye, Palo Alto Networks, and Imperva), though the process of preventing intrusions is a never-ending game of cat and mouse that will likely never be won. Other opportunities could be in alternative forms of identification. Social security numbers were created in 1936 to track a person's work history, not to verify a person's identity. Security experts are pushing to replace social security numbers with biometric technologies such as static (fingerprint sensors and facial recognition), and behavioral (typing recognition, signature analysis, and voice identification). We would expect identity verification to evolve toward multi-factor authentication: using a mix of unique passwords, geolocations, biometrics, and verification on a second device such as a mobile phone. Among the public companies leading this effort are Symantec, EMC Corp, and CA Inc.

Finally, here are a few personal reminders:

- Consider alternatives to AOL and Hotmail, as they are particularly prone to hacks.
- Use a password manager like Dashlane or 1Password so that you do not re-use passwords. The problem with re-using passwords is that if a password is hacked once, every site you've used it on is vulnerable.
- Freeze your credit. This is one of the best prevention measures you can take to protect yourself.
- Use a free credit-monitoring service. This gives you many of the advantages of a pay service, but without the cost.
- Sign on to your custodians, 401(k) provider, and other financial sites and complete your profile. This will prevent someone else from stealing your identity, logging in, and creating a profile for you.

Manchester Capital Management takes identity security and fraud prevention extremely seriously. In 2016, we adopted a third-party host for our database information because their security firewalls provided us a greater level of confidence in the protection of client data. For certain transactions, as an additional layer of protection we require verbal confirmation by clients. Recently, after exhaustive research into secure email systems, we have selected a system for encrypting information transmitted by email to clients and are in the process of rolling out the procedure.

We will continue to monitor the ripples of the Equifax data breach and will keep you apprised of any developments that could affect your personal profile or investment portfolio.

ENDNOTES

[1] "We've Been Breached: Inside the Equifax Hack", The Wall Street Journal, September 18, 2017